UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/990,860	11/09/2001	James W. Kasper	062891.0668	2711

5073	7590	09/23/2005

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER
ABYANEH, ALI S

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 09/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

		Application No.	Applicant(s)
Office Action Summary		09/990,860	KASPER ET AL.
		Examiner	Art Unit	
		Ali S. Abyaneh	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>06-27-2001</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-39</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-39</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>09 November 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>08-04-2003</u>.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   The amendment received on 06-27-2005 has been entered and considered.

Claim 35 has been amended.

Response to Arguments

2.   Applicant's arguments with respect to claims 1-39 have been considered but

are moot in view of the new ground(s) of rejections.

3.   Claims 1-39 are presented for examination.

Information Disclosure Statement PTO-1449

4.   The Information Disclosure Statement submitted by applicant on 08-08-2003has

been considered. Please see attached PTO-1449.

Claim Rejections - 35 USC § 102

5.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6.   Claim 19-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Eva

Chen et al. (US Patent NO.5, 960,170).

Regarding Claim 19

Chen teaches a method for use in intrusion detection comprising:

providing a sensor having a plurality of defined signatures (column 3, lines 57-

59), communicating to sensor a desire to create a modified signature (column 6,

lines 41-42), receiving from the sensor data indicative of parameters and

associated values for the signature to be modified (column 7, lines 25-27) and

providing to the sensor a modified value for at least one of the parameters to

create a modified signature (column 7, lines 34-40).

Regarding claim 20

Chen teaches all limitation of the claim as applied to claim 19 above. Chen

furthermore teaches a method comprising storing data associated with the

modified signature in the sensor at a location separate from the associated

unmodified signature (column 17, lines 24-25).

Regarding claim 21

Chen teaches all limitation of the claim as applied to claim 20

Above. Chen furthermore teaches storing in the sensor the name, signature

identification number, and one or more parameters and associated values for the

modified signature (column 13, lines1- 23 and fig 4c).

Regarding claim 22

Chen teaches all limitation of the claim as applied to claim 19 above. Chen

furthermore teaches communicating to the sensor the name of an engine

associated with the signature (column 13, lines 1-23)

Regarding claim 23

Chen teaches all limitation of the claim as applied to claim 20 above. Chen

furthermore teaches storing plurality of parameter names and associated value

(column 13, lines1- 23 and fig 4c).

Regarding claim 24

Chen teaches all limitation of the claim as applied to claim 19 above. Chen

furthermore teaches a method further comprising selecting a signature to be

modified from the plurality of defined signatures (column 3, lines 28-35).

Regarding claim 25

Chen teaches all limitation of the claim as applied to claim 22 above. Chen

furthermore teaches a method comprising receiving a list indicative of all defined

signatures associated with the engine (column 3, lines 57-60).

Regarding Claim 26 and 27

Chen teaches all limitation of the claim as applied to claim 19 above. Chen
furthermore teaches a method, wherein providing a sensor having a plurality of
defined signatures comprises providing a sensor having a default data file
defining the defined signatures and updating the default file (column 7, lines 62-
67).

7.   Claim 35-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Vimal
Vaidya. (US Patent NO 6,279,113)

Regarding Claim 35

Vaidya teaches a system for intrusion detection, comprising: a sensor for
detecting possible network intrusions, the sensor comprising: at least one engine
(column 7, lines 1-24); and a means for storing default signatures with
parameter-value pairs associated with the default signatures (column 6, lines 53-
57) and user-defined signatures with parameter-value pairs associated with the
user-defined signatures for defining signature to be detected by the at least one
engine (column 3, lines 21-22).

Regarding Claim 36

Vaidya teaches a method for use in intrusion detection of network traffic
comprising: storing in a memory a signature definition associated with a
signature to be detected (column 6, lines 53-56), the signature definitions

comprising: an identifier for the signature; and one or more parameter-value pairs

associated with the signature (column 9, lines 47-49), each parameter-value pair

comprising a parameter name and associated parameter value (column 9, lines

49-60); and determining, based on the signature definition, the values that

associated parameters of network traffic must take to meet the signature (column

10, lines 45-67 and column 11, lines 1-15).

Regarding Claim 37, 38 and 39

Vaidya teach all limitation of the claim as applied to claim 36 above.

Vaidya furthermore teaches a method, further comprising storing a plurality of

signature definitions in a data file, each signature definition on a different line of

the data file (column 6, lines 53-57), signature definition comprising an engine

parameter and an associate name for the engine parameter and each signature

definition comprises an identification parameter preceding the signature (column

9 lines 47-61).

Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth
> in section 102 of this title, if the differences between the subject matter sought to be patented and the
> prior art are such that the subject matter as a whole would have been obvious at the time the invention
> was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

9.   Claims 1-6, 8, 10, 13, 28 and 31-34 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Vimal Vaidya. (US Patent NO 6,279,113) in view of Alan S. Perelson

et al. (US patent NO Re 36,417).

Regarding Claim 1

Vaidya teaches a method for intrusion detection of network traffic

comprising: storing a data file comprising data defining one or more signature

definition and one or more parameters and associated values (column8, lines 8-

36); and executing signature definitions to detect network traffic matching the

signature definition (column 6, lines 53-57). Vaidya does not explicitly teach

generating, for each of the one or more signature definitions, an **inspector**

instance based on the data file; and executing, for each of the one or more

signature definitions, the **generated inspector instance** to detect network traffic

matching the signature definition. However, in an analogous art Perleson teaches

generating an inspector instance and executing the generated inspector instance

to detect network traffic matching the signature definition (column 6, lines 6-24).

Therefore it would have been obvious to person having ordinary skill in the art at

the time the invention was made to modify the method disclosed by Vaidya to

include generating, for each of the one or more signature definitions, an inspector

instance based on the data file; and executing, for each of the one or more

signature definitions, the generated inspector instance to detect network traffic

matching the signature definition. This would have been obvious because person

having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to prevent the spread of viruses and detect the newly introduced viruses and furthermore to match the plurality of contiguous digital signal of the test file to the plurality of contiguous digital signals of the original file (column 2, lines 8-12).

Regarding Claim 28

Vaidya teaches a system for intrusion detection comprising: a sensor for detecting possible network intrusions, one or more engine groups each associated with one or more network detection engines (column 6, lines 57-67 and column 7, lines 1-11) a configuration handler comprising: a default signature file storing one or more signature definitions defining one or more respective default signatures for use by the sensor; and a user signature file storing a plurality of user-defined signatures for use by the sensor(column 6, lines 53-57); executable code based on either one of the stored default signatures or one of the stored user-defined signatures, the executable code operable to detect a network intrusion defined by the associated user-defined signature or the associated default signature (column 6, lines 11-13). Vaidya does not explicitly teach **generating an executable code.** However in an analogous art Perleson teaches generating an executable code to detect a network intrusion (column 6, lines 6-24). Therefor it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by

Vaidya to generate an executable code based on either one of the stored default

signatures or one of the stored user-defined signatures, the executable code

operable to detect a network intrusion defined by the associated user-defined

signature or the associated default signature. This modification would have been

obvious because person having ordinary skill in the art at the time the invention

was made would have been motivated to do so in order to prevent the spread of

viruses and detect the newly introduced viruses and furthermore to match the

plurality of contiguous digital signal of the test file to the plurality of contiguous

digital signals of the original file (column 2, lines 8-12).

Regarding Claims 2, 3 and 4

Vaidya and Perleson teach all limitation of the claim as applied to claim 1

above. Vaidya furthermore teaches a method comprising: storing user data file

comprising signature definitions, each modified signature definition comprising

signature identifier associating the modified signature definition with a

corresponding signature definition stored in the data file and for each signature

definition, data comprising: a signature identification number parameter and

associated value; a signature name and associated string; one or more

parameters and respective values defining characteristics of the signature

(column 9, lines 48-52) and each signature definition is stored in a separate line

of data file (column 6, lines 53-57). Perleson furthermore teaches generating,

revised inspector instance based the modified signature definition and

corresponding generated inspector instance (column 6, lines 6-24).

Regarding Claim 5

Vaidya and Perleson teach all limitation of the claim as applied to claim 2

above. Vaidya furthermore teaches a method, wherein the one or more modified

signature definitions comprises modified values for associated modified

parameters and no values indicative of the parameters in the corresponding

signature definition that are not modified. (column 3, lines 1-11)).

Regarding Claim 6

Vaidya and Perleson teach all limitation of the claim as applied to claim 1

above. Vaidya furthermore teaches a method, wherein the data file comprises a

file received from a sensor provider (column 6, lines 44-56).

Regarding Claim 8

Vaidya and Perleson teach all limitation of the claim as applied to claim 1

above. Vaidya furthermore teaches a method of receiving the data file at the

sensor configuration handler (column 6, lines 37-40).

Regarding Claim 10

Vaidya and Perleson teach all limitation of the claim as applied to claim 1

above. Vaidya furthermore teaches a method comprising: storing a user data file

comprising one or more user-defined signature definitions, each user-defined

signature definition comprising a signature identifier not associated with any of

the signature definitions in the data file (column 9, lines 48-52). Perleson

furthermore teaches generating, for each of the user-defined signature

definitions, an inspector instance based on the user defined signature (column 6,

lines 6-24).

Regarding Claim 13

Vaidya and Perleson teach all limitation of the claim as applied to claim 10

above. Perleson furthermore teaches a method automatically generating, for

each custom signature, executable code operable to detect intrusions associated

with the custom signature based on the generated executable code of an

associated default signature (column 6, lines 6-24

Regarding Claim 31

Vaidya and Perleson teach all limitation of the claim as applied to claim 28

above. Vaidya furthermore teaches a system, wherein handler further comprises

a user interface operable to: receive an identification of a signature to be

modified; the configuration provides a list of parameters and associated values

for the signature to be modified (column 9, lines 48-52). Perleson furthermore

teaches receiving revised values for one or more of the parameters; and write a

revised signature to the user-defined data file (column 6, lines 6-24).

Regarding Claim 32 and 33

Vaidya and Perleson teach all limitation of the claim as applied to claim 28

above. Vaidya furthermore teaches a system, wherein the configuration handler

further comprises a user interface operable to: provide a list of possible

parameters for a particular engine; receive a plurality of values for one or more of

the parameters to define a user-defined signature associated with the engine;

and parameters; write a user-defined signature to the user signature file and a

reader and dispatcher to read data from default and user signature file and

transmit to one or more engine (column 7, lines 11-30).

Regarding Claim 34

Vaidya and Perleson teach all limitation of the claim as applied to

claim 28 above. Vaidya furthermore teaches a system further comprising a

management console associated with the sensor and operable to communicate

configuration data to the configuration handler and receive configuration help

information from the configuration handler (column 7, lines 25-30).

10.   Claims 7 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Vimal Vaidya. (US Patent NO 6,279,113) in view of Alan S. Perelson et al. (US patent

NO Re 36,417), further in view of Smaha et al. (US patent NO 5,557,742).

Regarding Claim 7 and 9

        Vaidya and Perleson teach all limitation of the claim as applied to claim 1

and above. Vaidya and Perleson do not explicitly teach the **data file comprises**

a file generated by a user and receiving configuration data file from a user

and storing the received configuration data file in a user data file. However

in an analogous art Smaha teaches the data file comprises a file generated by a

user and storing the received configuration data file in a user data file (paragraph

3, lines 54-64 and fig 4). Therefore it would have been obvious to person having

ordinary skill in the art at the time the invention was made to modify the method

disclosed by Vaidya and Perleson to include generating the data file by a user

and storing the received configuration data file in a user data file. This would

have been obvious because person having ordinary skill in the art at the time the

invention was made would have been motivated to do so in order to enable the

user to control the input mechanism and load a set of selected misuses

(paragraph 9, lines 1-5)

11.   Claims 12 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Vimal Vaidya. (US Patent NO 6,279,113), in view of Alan S. Perelson (US Patent

NO Re.36, 417), further in view of Kavin J. Ziese (US Patent NO 6,484,315).

Regarding Claim 12 and 29

Vaidya and Perleson teach all limitation of the claim as applied to claim 10

and 28 above. Vaidya and Perleson do not explicitly teach **storing a customized**

signature file comprises storing modification of one or more of the default

signature and configuration handler comprising stored modification to the

default signatures. However, in an analogous art Ziese teaches storing a

customized signature file comprises storing modification of one or more of the

default signature and configuration handler comprising stored modification to the

default signatures (column 4, lines 51-67 and column 5, lines 1-2). Therefore it

would have been obvious to person having ordinary skill in the art at the time the

invention was made to modify the method disclosed by Vaidya and Perleson to

include storing modification of one or more of the default signature and

configuration handler comprising stored modification to the default signatures.

This would have been obvious because person having ordinary skill in the art at

the time the invention was made would have been motivated to do so in order to

dynamically distribute intrusion detection update.

12.   Claims 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vimal

Vaidya. (US Patent NO 6,279,113), in view of Alan S. Perelson (US Patent NO Re.36,

417), in view of Kavin J. Ziese (US Patent NO 6,484,315), further in view of Smaha et

al. (US patent NO 5,557,742).

Regarding Claim 30

                 Vaidya, Perleson and Ziese teach all limitation of the claim as applied to

29 above. Vaidya, Perleson and Ziese do not explicitly teach **the stored**

modifications are stored in the user signature file. However, in an analogous

art, Smaha teaches a system wherein the stored modifications are stored in the

user signature file (paragraph 3, lines 54-64 and fig 4). Therefore it would have

been obvious to person having ordinary skill in the art at the time the invention

was made to modify the method disclosed by Vaidya, Perleson and Ziese to

store the modifications in the user signature file. This would have been obvious

because person having ordinary skill in the art at the time the invention was

made would have been motivated to do so in order to enable the user to control

the input mechanism and load a set of selected misuses (paragraph 9, lines 1-5).

13.   Claims 11 and 14-18 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Vimal Vaidya. (US Patent NO 6,279,113) in view of Kavin J. Ziese (US Patent NO

6,484,315).

Regarding Claim 11

Vaidya teaches a method for use in intrusion detection comprising: storing a default signature file defining one or more default signatures (column 6, lines 53-56); storing a customized signature file defining one or more custom signatures (paragraph 3, lines 21-23); generating, for each of the one or more signatures defined in the default signature file, executable code operable to detect intrusions associated with the default signature (column 6, lines 11-14); executable code operable to detect intrusions associated with the custom signature (column 6, lines 11-14 and column 3, lines 21-23). Vaidya does not explicitly teach **Automatically generating, executable code operable to detect intrusions associated with the default signature** and generating, executable code operable to detect intrusions associated with the custom signature. However, in an analogous art, Zies teaches a method wherein the executable codes are automatically generated (column 4, lines 51-56). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Vaidya to include Automatically generating, executable codes for default and customize signature. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to update systems in several sites with no or minimal operator interaction (column 2, lines 42-44).

Regarding Claim 14

Vaidya and Zies teach all limitation of the claim as applied to claim 11

above. Zies furthermore teaches a method, wherein the one or more custom

signatures comprises modifications of the default signatures (column 3, lines 61-

67).

Regarding Claim 15

Vaidya and Zies teach all limitation of the claim as applied to claim 11

above. Zies furthermore teaches a method, wherein generating, for each of the

one or more default signatures, comprises generating executable code

associated with the default signature based on an inspector shell (column 4, lines

51-56).

Regarding Claim 16

Vaidya and Zies teach all limitation of the claim as applied to claim 15

above. Zies furthermore teaches a method, wherein the executable code

associated with the default signature is operable to compare a plurality of

parameter values to a plurality of parameter values defined by the default

signature (paragraph 5, lines 16-23).

Regarding Claim 17

Vaidya and Zies teach all limitation of the claim as applied to claim 11

above. Vaidya furthermore teaches a method, wherein the default signature file

comprises, for each default signature; a signature identification number

parameter and associated value; a signature name and associated string; and

one or more parameters and respective values defining characteristics of the

default signature (column 9, lines 48-52).

Regarding Claim 18

Vaidya and Zies teach all limitation of the claim as applied to claim 11

above. Vaidya furthermore teaches a method, wherein the custom signature file

comprises, for each signature; a signature identification number parameter and

associated value; a signature name and associated string; and one or more

parameters and respective values defining characteristics of the default signature

(column 9, lines 48-52 and column 3, lines 21-23).

References Cited, Not Used

14.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure:

1. U.S. Patent No. 6,928,549

This reference relates to a method of operating an intrusion detection

system that protects a computer system from intrusions by vandals such as

hackers.

2. U.S. Patent No. 6,725,377

This reference relates to a computer program product and method that modifies anti-intrusion software on a computer network.

Conclusion

15.　Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300 Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ali Abyaneh　A·A
Patent Examiner
Art Unit 2133
09/1016/05

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100